509, 876

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

04 OCT 2004

(43) Date de la publication internationale
9 octobre 2003 (09.10.2003)

PCT

(10) Numéro de publication internationale
WO 03/083645 A2

(51) Classification internationale des brevets[7] : G06F 7/72

(21) Numéro de la demande internationale :
PCT/FR03/01058

(22) Date de dépôt international : 3 avril 2003 (03.04.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/04117 3 avril 2002 (03.04.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gemenos, F-13420 Gemenos (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **JOYE, Marc** [BE/FR]; 19, rue Voltaire, F-83640 Saint Zacharie (FR). **CHEVALLIER-MAMES, Benoît** [FR/FR]; Résidence Le Général, 14, boulevard Ganteaume, F-13400 Aubagne (FR).

(74) Mandataire : **BRUN, Philippe**; c/o Gemplus, Service brevets, La Vigie, PB 90, F-13705 La Ciotat Cedex (FR).

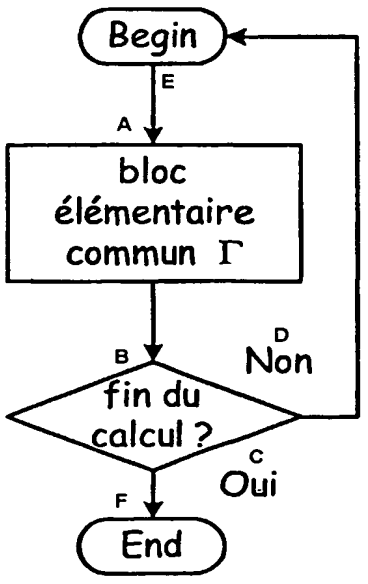
(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,

[Suite sur la page suivante]

(54) Title: CRYPTOGRAPHIC METHOD PROTECTED AGAINST COVERT CHANNEL TYPE ATTACKS

(54) Titre : PROCEDE CRYPTOGRAPHIQUE PROTEGE CONTRE LES ATTAQUES DE TYPE A CANAL CACHE



A...BLOC ÉLÉMENTAIRE COMMUN:- COMMON ELEMENTARY BLOCK
B...FIN DE CALCUL?:- END OF CALCULATION?
C...OUI:- YES
D...NON:- NO
E...DEBUT
F...FIN

(57) Abstract: The invention relates to a cryptographic method secured against a covert channel attack. According to the invention, in order to carry out a selected block of instructions (?j) as a function of an input variable (D_1) amongst N predefined instruction blocks (?1,, ?<SB>N</SB>), a common block (Γ (k,s)) is carried out on the predefined N instruction blocks (?1,, ?<SB>N</SB>), a predefined number (L_j) of times, the predefined number (L_j) being associated with the selected instruction block (?j).

(57) Abrégé : L'invention concerne un procédé cryptographique sécurisé contre une attaque à canal caché. Selon l'invention, pour exécuter un bloc d'instructions choisi (Πj) en fonction d'une variable d'entrée (D_1) parmi N blocs d'instructions prédéfinis (Π_1, , Π_N), on exécute un nombre prédéfini (L_j) de fois un bloc commun ((k,s)) aux N blocs d'instructions prédéfinis (Π_1, , Π_N), le nombre prédéfini (L_j) étant associé au bloc d'instructions choisi (Π_j).

WO 03/083645 A2